Journal of Social Research

**JOSR: Journal of Social Research**
**April 2022, 1 (5), 318-327**

p-ISSN: 2827-9832 e-ISSN: 2828-335x

Available online at http:// https://ijsr.internationaljournallabs.com/index.php/ijsr

# PERANCANGAN DAN IMPLEMENTASI ANALISIS KEAMANAN NIDS SISTEM NOTIFIKASI ROUTEROS MENGGUNAKAN PESAN INSTAN DI JARINGAN CLOUD PUBLIK

**Ekky Rega Prabowo, Marza Ihsan Marzuki**

Electrical Engineering Mercu Buana University, Jakarta, Indonesia
prabowo.eki@gmail.com, im.marza@gmail.com

Received: 1 April 2022
Revised : 5 April 2022
Accepted: 8 April 2022

**Abstrak**

Serangan siber memiliki dampak signifikan pada kinerja jaringan di cloud publik. Sysadmin harus siap untuk menangani setiap serangan di server yang sangat dibutuhkan untuk mencegah serangan yang dapat mengganggu kinerja jaringan cloud publik. Diperlukan suatu sistem untuk mendeteksi dan memberikan peringatan dini terhadap setiap serangan siber. Oleh karena itu, diperlukan sistem yang secara otomatis mengirimkan notifikasi kepada administrator secara real-time dengan memanfaatkan platform Instant Messaging. Makalah ini memberikan analisis terhadap sistem notifikasi yang dibangun menggunakan RouterOS sebagai NIDS dengan Instant Messaging sebagai platform notifikasi, yaitu serangan IcmpFlooding, PortScanning, dan HttpFlooding. Hasil yang diperoleh menunjukkan bahwa sistem berhasil memberikan notifikasi berupa waktu serangan, IP sumber serangan, sumber port serangan dan jenis serangan secara real-time. Hal ini diharapkan dapat membantu sysadmin melakukan tindakan penanganan selanjutnya terhadap ancaman di jaringan cloud publik.

**Kata kunci**: RouterOS; NIDS; Cloud Publik; Pesan Instan

***Abstract***

*Cyber attacks have a significant impact on network performance in public clouds. Sysadmins must be prepared to handle any attack on the server that is urgently needed to prevent attacks that can disrupt the performance of public cloud networks. a system is needed to detect and provide early warning of any cyber attacks. Therefore, the required system automatically sends notifications to administrators in real-time by making use of the Instant Messaging platform. This paper provides an analysis of the notification system built using RouterOS as NIDS with Instant Messaging as the notification platform, namely IcmpFlooding, PortScanning, and HttpFlooding attacks. The results obtained indicate that the system has succeeded in providing notifications in the form of attack time, attack source IP, attack source port and attack type in real-time. This is expected to help sysadmins take further action against threats on public cloud networks.*

***Keyword**s: RouterOS; NIDS; Public Cloud; Instant Messaging*

**Correspondent Author : Ekky Rega Prabowo*
*Email : prabowo.eki@gmail.com*



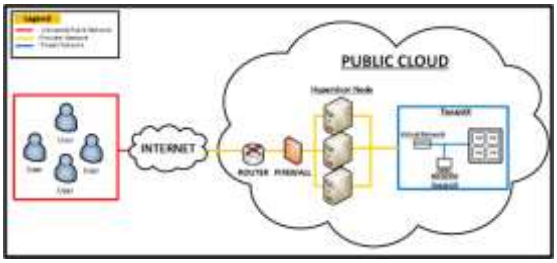
## PENDAHULUAN

Awal era industri 4.0 terlihat kemajuan yang sangat pesat dalam dunia Cloud Computing. Cloud Computing telah menyediakan berbagai sumber daya seperti penggunaan sumber daya, penyimpanan, dan aplikasi kepada pengguna melalui Internet. Penyedia layanan komputasi awan di pasar Indonesia saat ini antara lain AWS, Google, IBM, Microsoft, Salesforce dan Biznet Gio Cloud (Aldeen, Salleh, & Razzaque, 2015). Menurut (Freet, Agrawal, John, & Walker, 2015) yang telah menjelaskan buku (Badger, Grance, Patt-Corner, & Voas, 2012) bahwa "Public Cloud IaaS mengandalkan jaringan yang aman dan andal, serta browser yang aman untuk administrasi akun.


**Gambar I**
**Berbagi Tanggung Jawab Keamanan**
(Sumber: The Shared Responsibility Model for Cloud Security | CloudCheckr, n.d.)

Harap dicatat bahwa penyedia cloud untuk keamanan platform, perangkat lunak dan aplikasi yang digunakan adalah tanggung jawab pengguna. Pada saat yang sama, penyedia cloud hanya bertanggung jawab dalam hal infrastruktur. Oleh karena itu, untuk menggunakan layanan cloud membutuhkan pengalaman yang terampil dan ahli di bidang IT.

Menurut (Lindemann, 2015) "Secara default, sistem keamanan yang disediakan oleh penyedia cloud computing hanya firewall, sedangkan tindakan teknis dan non-teknis dapat berperan dalam mencegah penyalahgunaan.




**Gambar 2**
**IDS Topologi Implementasi di Cloud Publik**

Kemudian (Chiba, Abghour, Moussaid, El Omri, & Rida, 2016) menjelaskan bahwa IDS adalah proses monitoring event yang terjadi pada sistem atau jaringan public cloud kemudian menganalisanya untuk mencari intervensi. IDS dapat berupa perangkat lunak, perangkat keras, atau kombinasi keduanya yang memantau aktivitas berbahaya atau pelanggaran kebijakan.

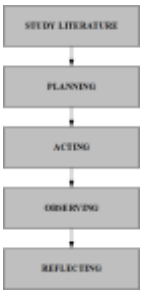
Untuk dapat menerapkan IDS membutuhkan perangkat RouterOS. Memiliki beberapa router antara lain : Vyatta, Sucirata, Snort, Mikrotik, Cisco dan lain-lain. Tapi yang memiliki kualitas tingkat tinggi dan user friendly hanya Cisco, Mikrotik (Kurniawan, Nabiila Putri, & Hermanto, n.d.).

Penelitian sebelumnya (Cropper, Ullrich, Frühwirt, & Weippl, 2015) menjelaskan bahwa meskipun dasar, fungsionalitas firewall dapat ditambah dengan pengaturan keamanan yang sesuai dengan kebutuhan klien. Sedangkan pada penelitian lain menggunakan fitur automata analyze yang dilakukan oleh (Probst, Alata, Kaâniche, & Nicomette, 2015) dengan menggunakan aplikasi Wireshark sebagai media monitoring permintaan trafik dari server yang dimonitor, namun tetap diperlukan upaya administrator sistem untuk dapat melakukan check in secara hidup.

Berdasarkan referensi di atas, maka perlu adanya peningkatan keamanan di cloud publik karena masih terdapat kekurangan pada standar keamanan yang diberikan oleh penyedia cloud. Pada penelitian, penulis merancang dan mengimplementasikan IDS di cloud publik dan menambahkan media aplikasi pesan instan sebagai sistem notifikasi ke sistem administrator.

## METODE PENELITIAN

Penelitian ini terdiri dari beberapa tahapan yang ditunjukkan pada Gambar III-1; setiap langkah memiliki alur penelitian yang mengantarkan masalah penelitian ke tujuan penelitian.




Gambar 3
Tahapan Metodologi

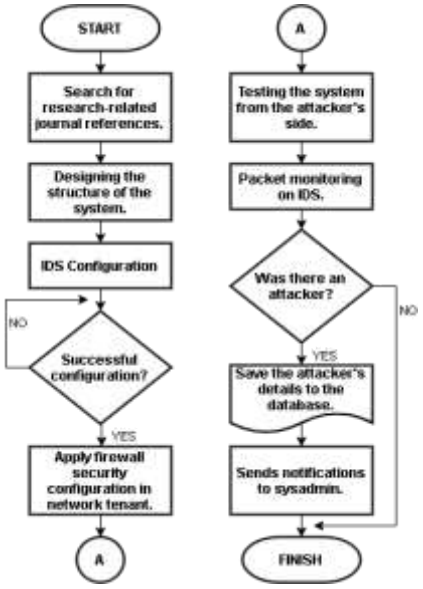
**A. Studi literatur**

Tahap ini penulis mencari literatur, jurnal internasional, buku-buku di Google Scholar dan Publikasi – IEEE mengenai sistem jaringan yang akan dibangun (IDS, RouterOS, tabel IP, keamanan cloud, dan lain-lain), dan mulai mempelajari teori-teori pendukung dalam literatur.Planning

Penulis mengidentifikasi masalah/ancaman utama dalam literatur yang telah dikumpulkan kemudian menganalisis kekurangannya, setelah itu dilakukan tahap selanjutnya antara lain:

- Desain perangkat keras dan perangkat lunak
- Sistem Desain

Pada perancangan, rancangan flowchart menjelaskan alur implementasi IDS yang terintegrasi dengan instant messaging yang diteliti pada gambar III-2.




**Gambar 4**
**Flowchart implementasi sistem IDS di Public Cloud**

**1. Akting**

Setelah mempelajari teori pendukung dan merancang desain penelitian. Selanjutnya, ada beberapa skenario, antara lain:

- Penciptaan penyerang VM, IDS, dan VM target serta aplikasi pesan instan sebagai objek penelitian.
- Konfigurasi keamanan data.

Setelah tahap implementasi dilanjutkan dengan proses pengujian sistem keamanan yang telah dibuat oleh penulis dengan melakukan berbagai skenario pengujian sebagai berikut :

- Pengujian sistem dengan berbagai teknik serangan seperti Icmp Flood, Port Scanning, dan HTTP Flood.
- Integrasikan pemantauan peringatan secara real-time kepada administrator.

**a. Mengamati**

Setelah diterapkan dan diuji, penulis mengevaluasinya kemudian membandingkannya dengan penelitian terkait.

**b. Mencerminkan**

Penulis kemudian mengevaluasi setiap tahapan kinerja dan hasil dalam implementasinya. Yang kemudian memberikan kesimpulan, kelebihan dan kekurangan yang telah penulis bangun.

## HASIL DAN PEMBAHASAN

### A. Hasil Penelitian

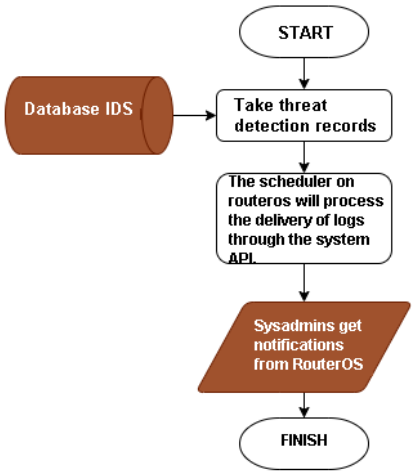
Pada bagian ini dijelaskan prosedur dan hasil selama penelitian berdasarkan penjelasan metodologi, antara lain:

- IDS skenario implementasi terintegrasi dengan pemberitahuan peringatan.
- 10x skenario pengujian sistem keamanan untuk mendapatkan hasil sistem peringatan secara realtime.
- Analisis hasil tes.

**A. IDS skenario implementasi terintegrasi dengan notifikasi peringatan.**

Pada tahap ini dijelaskan langkah-langkah yang akan dilakukan untuk integrasi yaitu: persiapan, konfigurasi dan integrasi.

- Persiapan
  Akan dilakukan pembuatan semua komponen yang diperlukan, termasuk membangun lingkungan VM dan layanannya, Membuat bot alert di aplikasi instant messaging.
- Konfigurasi
  Setelah proses persiapan selesai maka langkah selanjutnya adalah melakukan konfigurasi keamanan data pada RouterOS.
- Integrasi
  Setelah semua konfigurasi diatur berdasarkan aturan masing-masing akan dilakukan integrasi RouterOS dengan aplikasi instant messaging bertujuan ketika mendeteksi ancaman dapat memberikan peringatan dini pada sys admin dijelaskan pada gambar IV-1:




**Gambar 5**
**Flowchart mengirim peringatan ke administrator**

**B. Skenario pengujian sistem keamanan dalam 10x percobaan untuk mendapatkan hasil sistem peringatan waktu nyata.**

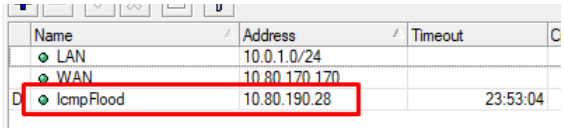
Pengujian sistem ini merupakan langkah untuk mengetahui seberapa besar tingkat beban yang akan diuji dan diterima dari serangan VM ke VM target. Berikut beberapa serangannya:

- Icmp Serangan Banjir

Penulis menggunakan dua tools yaitu manual ping, dengan request secara simultan maka menggunakan tools ping flood. Setelah serangan RouterOS akan mendeteksi dan mengirimkan notifikasi ke instant messaging, seperti pada gambar IV-2:


**Gambar 6**
**Icmp Notifikasi Waspada Banjir**

Kemudian RouterOS menyimpan log alamat IP untuk memudahkan administrator sistem untuk melakukan tindakan selanjutnya pada penyerang seperti pada gambar IV-3:




**Gambar 7**
**Log IP Alamat IcmpFlood**

Serangan dilakukan sebanyak 10x untuk mengetahui rata-rata waktu yang dibutuhkan setiap serangan yang ditangani oleh RouterOS kemudian dikirimkan dengan instant messaging, dan didapatkan hasil waktu pada serangan pertama adalah 23 detik, 2nd 18 detik, 3rd, 20 detik, 4th , 21 dtk, 24 dtk ke-5, dtk ke-6 23, dtk ke-7 22, dtk ke-8 26, dtk ke-9 15 dan dtk ke-10 dijelaskan pada gambar IV-4.:

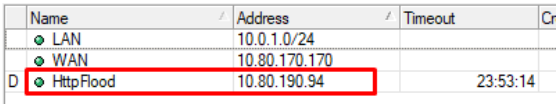

**Gambar 8**
**Grafik waktu notifikasi percobaan ICMP Flood 10x**

- **HTTP Serangan Banjir**

Tahap ini, penulis akan meminta HTTP ke VM target menggunakan tool benchmark apache.
Setelah serangan RouterOS akan mendeteksi dan mengirimkan notifikasi ke instant messaging, seperti pada gambar iv-5:


**Gambar 9**
**Notifikasi Peringatan HttpFlood**

Kemudian RouterOS menyimpan log alamat IP untuk memudahkan administrator sistem melakukan tindakan selanjutnya pada penyerang seperti pada gambar IV-6:



| | Name | Address | Timeout | Cr |
|---|---|---|---|---|
| | LAN | 10.0.1.0/24 | | |
| | WAN | 10.80.170.170 | | |
| D | HttpFlood | 10.80.190.94 | 23:53:14 | |

**Gambar 10**
**Log IP Alamat HttpFlood**

Serangan dilakukan 10x untuk mengetahui rata-rata waktu yang dibutuhkan setiap serangan yang ditangani oleh RouterOS kemudian dikirimkan dengan instant messaging, dan didapatkan hasil waktu serangan pertama adalah 32 detik, 2nd 36 detik, 3rd, 33 detik, 4th, 30 detik, 34 detik ke-5, 25 detik ke-6, 31 detik ke-7, 26 detik ke-8, ke-28 detik dan ke-10 23 detik dijelaskan pada gambar IV-7:


**Gambar 11**
**Grafik waktu notifikasi dalam uji coba HTTP Flood 10x**

- **Serangan Pemindaian Port**

  Serangan ini akan dilakukan dengan menggunakan dua alat yang hampir mirip, tetapi sistem operasi yang berbeda, yaitu Nmap dan Zenmap, akan dilakukan melalui os Linux dan Zenmap dilakukan dengan menggunakan aplikasi desktop windows. Setelah serangan RouterOS mendeteksi dan mengirimkan notifikasi ke instant messaging, seperti Gambar IV-8:


**Gambar 12**
**Pemindaian Port Notifikasi Peringatan**

Kemudian RouterOS menyimpan log alamat IP untuk memudahkan administrator sistem untuk melakukan tindakan selanjutnya pada penyerang seperti pada Gambar IV-9:

| | Name | Address | Timeout | Cr |
|---|---|---|---|---|
| | LAN | 10.0.1.0/24 | | |
| | WAN | 10.80.170.170 | | |
| D | PortScanner | 10.80.190.94 | 23:57:15 | |

**Gambar 13**
**Log IP Pemindaian Port Alamat**

Serangan dilakukan 10x untuk mengetahui rata-rata waktu yang dibutuhkan setiap serangan yang ditangani oleh RouterOS kemudian dikirimkan dengan instant messaging, dan didapatkan hasil waktu pada serangan pertama adalah 27 detik, 2nd 24 detik, 3rd, 23 detik, 4th, 25 dtk, 30 dtk ke-5, 20 dtk ke-6, dtk ke-7 28, dtk ke-8 27, dtk ke-9 dan dtk ke-10 dijelaskan pada Gambar IV-10:


**Gambar 14**
**Grafik waktu pemberitahuan dari percobaan Pemindaian Port 10x**

## B. Pembahasan

### A. Hasil Uji Analisis

Hasil pada tahap pengujian 3 serangan yang dilakukan pada target VM setelah implementasi id di public cloud dan terintegrasi dengan aplikasi instant messaging menghasilkan informasi antara lain:

**Tabel 0-1**
**Analisis Pengujian**

| Types | of | Detectio | Notificatio | Average |
|---|---|---|---|---|

| Attacks | n Success Rate | n received Rate | Notificatio n Received Timing |
|---|---|---|---|
| ICMP Flood | 100% | 100% | 21.5 Seconds |
| HTTP Flood | 100% | 100% | 29.8 Seconds |
| Port Scanning | 100% | 100% | 26 Seconds |

Port Scanning 100% 100% 26 Seconds Berdasarkan tabel IV-1 hasil pengujian yang telah dilakukan dapat dianalisa bahwa setiap rule yang telah dikonfigurasi oleh RouterOS dapat mendeteksi ancaman yang dikirim dan mampu menyimpan history log alamat IP penyimpanan yang lama tergantung kebutuhan administrator sistem. Kemudian dari konfigurasi tagging yang telah dilakukan dari setiap rule, system administrator dapat mengetahui jenis serangannya.

Berdasarkan hasil analisis respon waktu pengiriman notifikasi yang dilakukan dalam percobaan 10x, setiap serangan diperoleh hasil yang mendekati realtime, antara lain ICMP Flooding 21,5 detik, Port Scanning 26 detik, dan HTTP Flooding 29,8 detik.

Dalam Sistem Manajemen Keamanan Informasi (SMKI) / ISO 27001:2013 poin A.13.1.1 Standar Kontrol Jaringan dijelaskan dalam (kontrol jaringan ISO 27001: Sistem Deteksi Intrusi & Honeypots, n.d.). Jaringan organisasi harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi untuk meminimalkan jendela waktu bagi peretas untuk mendapatkan keuntungan dari tindakannya. Serta pada pedoman pelaksanaan poin (d) "pencatatan dan pemantauan yang tepat harus diterapkan untuk memungkinkan perekaman dan deteksi tindakan yang dapat mempengaruhi atau relevan dengan keamanan informasi."

## KESIMPULAN

Penelitian yang dilakukan oleh penulis adalah merancang dan menguji sistem yang dapat mengirimkan notifikasi peringatan NIDS kepada administrator secara real-time dengan memanfaatkan instant messaging pada jaringan pengguna pada public cloud, sysadmin mampu menyadari beberapa ancaman yang sedang atau telah terjadi di lingkungan jaringan yang dikelolanya. Mengacu pada aturan konfigurasi di RouterOS yang dapat mengidentifikasi berbagai jenis aktivitas intervensi seperti IcmpFlood, PortScanning, HttpFlood dan dapat mengetahui IP Address penyerang, yang kemudian disimpan dengan melakukan tagging sesuai dengan jenis serangan yang telah terpasang.
Respon waktu pengiriman notifikasi yang dilakukan dalam iterasi 10x setiap serangan diperoleh hasil rata-rata 21,5 detik untuk IcmpFlooding, 26 detik untuk PortScanning, dan 29,8 detik untuk HttpFlooding. Penelitian ini termasuk dalam standar Kontrol Jaringan ISO 27001:2013 poin A.13.1.1 yang dijelaskan dalam (kontrol jaringan ISO 27001: Intrusion Detection System & Honeypots, n.d.), IDS dan notifikasi peringatan mendeteksi dan memberikan peringatan yang valid dan realtime untuk meminimalkan peretas tindakan lebih lanjut dan membantu meningkatkan kesadaran sysadmin terhadap ancaman terhadap jaringan di cloud publik.

## BIBLIOGRAFI

Aldeen, Yousra Abdul Alsahib S., Salleh, Mazleena, & Razzaque, Mohammad Abdur. (2015). A survey paper on privacy issue in cloud computing. *Research Journal of Applied Sciences, Engineering and Technology*, *10*(3), 328–337. Google Scholar

Badger, Mark Lee, Grance, Timothy, Patt-Corner, Robert, & Voas, Jeffery M. (2012). *Cloud computing synopsis and recommendations*. National Institute of Standards & Technology. Google Scholar

Chiba, Zouhair, Abghour, Noureddine, Moussaid, Khalid, El Omri, Amina, & Rida, Mohamed. (2016). A survey of intrusion detection systems for cloud computing environment. *2016 International Conference on Engineering & MIS (ICEMIS)*, 1–13. IEEE. Google Scholar

Cropper, Jordan, Ullrich, Johanna, Frühwirt, Peter, & Weippl, Edgar. (2015). The role and security of firewalls in iaas cloud computing. *2015 10th International Conference on Availability, Reliability and Security*, 70–79. IEEE. Google Scholar

Freet, David, Agrawal, Rajeev, John, Sherin, & Walker, Jessie J. (2015). Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. *Proceedings of the 7th International Conference on Management of Computational and Collective IntElligence in Digital EcoSystems*, 148–155. Google Scholar

Kurniawan, Adhitya, Nabiila Putri, Sayyidah, & Hermanto, Dedy. (n.d.). *IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT, IP TABLES, DAN HONEYPOT PADA ROUTER MIKROTIK*. Google Scholar

Lindemann, Jens. (2015). Towards abuse detection and prevention in IaaS cloud computing. *2015 10th International Conference on Availability, Reliability and Security*, 211–217. IEEE. Google Scholar

Probst, Thibaut, Alata, Eric, Kaâniche, Mohamed, & Nicomette, Vincent. (2015). Automated evaluation of network intrusion detection systems in iaas clouds. *2015 11th European Dependable Computing Conference (EDCC)*, 49–60. IEEE. Google Scholar

The Shared Responsibility Model for Cloud Security | CloudCheckr. (n.d.). Google Scholar